



January 30, 2023

TO: Members, Subcommittee on Innovation, Data, and Commerce
FROM: Committee Majority Staff
RE: Hearing Entitled “Economic Danger Zone: How America Competes to Win the Future Versus China”

I. INTRODUCTION

The Subcommittee on Innovation, Data, and Commerce will hold a hearing on Wednesday, February 1, 2023, at 10:30 a.m. in 2322 Rayburn House Office Building. The hearing is entitled “Economic Danger Zone: How America Competes to Win the Future Versus China.”

II. WITNESSES

- Brandon Pugh, Policy Director and Resident Senior Fellow, R Street Institute
- Jeff Farrah, Executive Director, Autonomous Vehicle Industry Association (AVIA)
- Samm Sacks, Cyber Policy Fellow, International Security Program, New America
- Marc Jarsulic, Senior Fellow and Chief Economist, Center for American Progress

III. BACKGROUND

Since our country’s founding, the United States has faced challengers and challenges in many forms. We have experienced economic recessions and revolutions, and each time the U.S. has relied on its people and an entrepreneurial private sector to bounce back and innovate. Today, the U.S. is on the edge of a new challenge – the fight for global leadership in the age of emerging technology.

Today’s main challenges are digital and technological, with the leading countries writing the rules for those lagging behind. As the world transitioned towards online technologies and services, many countries enacted privacy and data security rules to dictate the usage and collection of personal information. The countries that act first, when it comes to state encouragement and building a framework for operation and adoption, often write the rules of the road based on their values and become the dominant player in that field. The Chinese Communist Party (CCP) has taken advantage of this strategy, enacting both the Personal Information Protection Law and Data Security Law in 2021. These laws drastically impact how companies, that operate in China, must treat their citizen’s personal information domestically and

abroad.¹ Privacy and data security laws provide an important framework and regulatory certainty needed for industry to invest in and to deploy emerging technologies.

In recent years, the CCP has doubled down on its intent to become the global leader in the deployment of emerging technologies by directing government resources and human capital towards this goal. To bolster itself as a legitimate global leader, the CCP parliament passed an initiative to invest and consolidate resources for scientific and technological national laboratories with a focus on researching and developing emerging technologies.² This includes artificial intelligence (AI) and its many applications like autonomous vehicles (AVs), quantum computing, additive manufacturing, internet of things (IOT), blockchain, and other emerging technologies.

Given the CCP's increased momentum for global technological dominance, the Committee seeks to reassert the need for Congress to establish foundational frameworks, such as a federal privacy and data security law and standards deployment and commercialization, that underpin our efforts to lead on deploying emerging technologies, such as autonomous vehicles. This hearing will examine, in the absence of U.S. action in these spaces, the clear and present dangers of relinquishing leadership to China.

A. THE THREAT TO AMERICAN LEADERSHIP

In December 2021, the CCP's Central Commission for Cybersecurity and Information issued its 14th Five-Year Plan. This plan outlines China's ambitions to become the global leader in the digital economy by 2025.³ For the CCP, global tech leadership is seen as a required component for its economic and political survival.⁴

As extensively documented by media reports, the CCP has used the religious and ethnic minorities of the Xinjiang Uyghur Autonomous Region as fuel for the development of its technologically powered surveillance state.⁵ In Xinjiang, China created a Joint Operations Platform which integrated iris scanners, CCTV cameras, and DNA sampling to build advanced facial and voice recognition algorithms.⁶ These algorithms are no longer confined exclusively to

¹ Ryan Junck, et. al., *China's New Data Security and Personal Information Protection Laws: What they Mean for Multinational Companies*, Skadden (November 3, 2021).

<https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws>

² Ben Murphy, *Translation: Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035*, CSET (May 12, 2021).

https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf

³ Rogier Creemers, et. Al., *Translation: 14th Five-Year Plan for National Informatization* (December 2021).

<https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/>

⁴ U.S.-China Economic and Security Review Commission, *2021 Annual Report to Congress* (November 2021)

Available at: https://www.uscc.gov/sites/default/files/2021-11/2021_Annual_Report_to_Congress.pdf

⁵ U.S. Department of State, *Determination of the Secretary of State on Atrocities in Xinjiang* (January 19, 2021).

<https://2017-2021.state.gov/determination-of-the-secretary-of-state-on-atrocities-in-xinjiang/index.html>

⁶ Jacky Habib, *In Xinjiang, China, Surveillance technology is used to help the state control its citizens*, CBC.

<https://www.cbc.ca/passionateeye/features/in-xinjiang-china-surveillance-technology-is-used-to-help-the-state-control>

Xinjiang, using an enslaved people to advance the technology, but now are being integrated into the millions of surveillance cameras throughout mainland China.⁷ Declines in camera prices and data storage, when combined with the CCP's blatant disregard for civil liberties, has enabled Chinese tech companies to rapidly advance and surpass countries who value human rights.⁸

Whenever it can, the CCP undermines the U.S.-led international order, by helping nations like Russia and North Korea evade sanctions.⁹ Throughout the developing world, China is building its presence and influence by creating a coalition of anti-Western sentiment. In a 2015 whitepaper, the CCP highlighted the role of building a China-led global governance regime which aims to achieve “comprehensive reform” to the current international system.¹⁰ The whitepaper outlines how Chinese exports – law enforcement, riot control, infrastructure, cyberspace management, science, and technology – can strengthen relationships with African partners.¹¹

Maintaining and securing U.S. leadership in technology is essential for U.S. growth, security, and competitiveness in the 21st century. Michael Kratsios, former U.S. Chief Technology Officer, has said that technological leadership from democratic nations has “never been more imperative. If we want to make sure that Western values are baked into the technologies of the future, we need to make sure we’re leading in those technologies.”¹² The innovation, standard setting, and deployment of new and emerging technologies by CCP creates a risk for the U.S.

B. DATA PRIVACY AND PROTECTION IN THE CCP

CCP-controlled digital products, from Tencent-owned WeChat to ByteDance-owned TikTok, are growing in popularity around the world, including in the U.S. These applications give the CCP access to our most sensitive information, including our precise geolocation, online patterns, and our private conversations. The collection of such information has sparked questions over how algorithms are developed by Chinese engineers. While these products are nominally controlled by private entities, they are de facto arms of the CCP through a complex web of laws and policies which compel organizations to carry out the wishes of the CCP.¹³ To show how far this web of laws and policies can reach, in 2019 a 17-year old American, located in the U.S., was

⁷ Ross Anderson, *The Panopticon is Already Here*, The Atlantic (September 2020)

<https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/>

⁸ Yael Grauer, *Revealed: Massive Chinese Police Database*, The Intercept (January 29, 2021).

<https://theintercept.com/2021/01/29/china-uyghur-muslim-surveillance-police/>

⁹ James Areddy, *China Opposes Sanctions and Has a Reputation for Busting Them*, WSJ (March 6, 2022)

<https://www.wsj.com/articles/china-opposes-sanctions-and-has-a-reputation-for-busting-them-11646562600>

¹⁰ Xinhua, *Full Text: China's Second Africa Policy Paper* (December 5, 2015).

http://www.chinadaily.com.cn/world/XiattendsParisclimateconference/2015-12/05/content_22632874.htm.

¹¹ Ibid.

¹² Ross Anderson, *The Panopticon is Already Here*, The Atlantic (September 2020)

<https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/>

¹³ China Law Translate, *PRC National Intelligence Law (as amended in 2018)*, (March 17, 2021).

<https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>

suspended from TikTok for posting a video in which she talked about atrocities occurring in Xinjiang.¹⁴

In 2021, the CCP began to crack down on non-state technology and e-commerce companies by launching a series of investigations, issuing significant penalties, and introducing new regulations. According to *Trivium China*, establishing state control over consumer data and exerting more direct control of non-state actors was a key driver of this crackdown.¹⁵

While China has passed two consumer data privacy laws, they are anything but pro-consumer. Their laws have reinforced China's mercantilist data strategy – increase CCP access to data, both foreign and domestic, while limiting external access to data.¹⁶ China's development of a data governance regime is part of larger strategy to influence global data norms, policies, and standards.¹⁷ China's approach to data, which encourages cyber-sovereignty and local data storage, is concerning to many human rights experts and U.S. tech firms.¹⁸

To remain competitive, the U.S. must ensure there are guardrails around any data sharing with Chinese companies. The U.S. must seek out business environments and partners that share our values. Failure to do so leaves U.S. data available to Chinese companies seeking to use the information for a variety of purposes, which will result in the U.S. leadership being compromised.

C. DATA PRIVACY AND PROTECTION IN THE UNITED STATES

Last Congress, the House Committee on Energy and Commerce took a major step forward to establish a national privacy and data security law when it passed H.R. 8152, the bipartisan and bicameral American Data Privacy and Protection Act (ADPPA), out of committee 53-2.

The ADPPA would establish strong data security requirements for companies and limit the type of information that certain companies can collect, transfer, and process. These safeguards ensure Americans have more control over their sensitive information and includes robust privacy protections for all Americans. ADPPA would also specifically add protections relative to China by requiring that any company that collects personal information must disclose to the individual to which the data pertains, that their information is sent to, transferred, or otherwise made available to China, as well as other foreign threats including Russia, North Korea, and Iran.

¹⁴ Drew Harwell and Tony Romm, *A 17-year-old posted to TikTok about China's detention camps. She was locked out of her account*, (November 26, 2019). <https://www.washingtonpost.com/technology/2019/11/26/year-old-posted-tiktok-about-chinas-detention-camps-her-account-was-suspended/>

¹⁵ Trivium China, *Deep Dive: China's Triple Tech Crackdown*, (July 2, 2021). <https://triviumchina.com/2021/07/12/in-depth-chinas-triple-tech-crackdown/>

¹⁶ U.S.-China Economic and Security Review Commission, *China's Evolving Data Governance Regime*, (July 26, 2022) https://www.uscc.gov/sites/default/files/2022-07/Chinas_Evolving_Data_Governance_Regime.pdf

¹⁷ Graham Webster, *Translation: Data Security Law of the People's Republic of China*, DigiChina (June 29, 2021). <https://digichina.stanford.edu/news/translationdata-security-law-peoples-republic-china>.

¹⁸ Shannon Tiezzi, *China's Bid to Write the Global Rules on Data Security*, The Diplomat (September 10, 2020). <https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/>

In the absence of Congressional action, State legislatures have established privacy and data security laws. However, the confusion and compliance burden arising from the patchwork of state laws emphasizes the need for Congress to pass a preemptive federal privacy and data security standard. This piecemeal approach hurts the U.S. stature on the world stage. A failure to do so creates barriers for innovative U.S. based start-ups and small businesses. If small businesses are forced to comply with potentially 50 conflicting state laws, it further stunts the growth of their business and their ability to deploy new technologies for Americans.

The U.S. must ensure that it passes a federal privacy and data security standard, like ADPPA, providing regulatory certainty and a lower compliance burden for new market entrants and incumbents. Chinese companies, who enjoy a nationalized privacy and data security standard, operate with this regulatory certainty, which is a competitive edge.

D. EMERGING TECHNOLOGY

a. ARTIFICIAL INTELLIGENCE

As an emerging field, AI is a broader term that can be broken down into many different subfields with recognizable real-world applications:

Broad Term	Subfield	Real-World Application
Artificial Intelligence	<i>Supervised Learning</i>	<ul style="list-style-type: none">- Personalizing social media feeds- Creating show, movie, and video recommendations- Sorting, tagging, and categorizing photos
	<i>Reinforcement Learning</i>	<ul style="list-style-type: none">- Holding, buying, or selling stocks- Dynamic disease treatment regimes- Control of passive heating and cooling in buildings
	<i>Natural Language Processing</i>	<ul style="list-style-type: none">- Email filtering- Language translation- Online search engines- Smart assistants
	<i>Computer Vision</i>	<ul style="list-style-type: none">- Cars identify objects in their surroundings- Facial recognition- Deepfake detection

Governments around the world have started investing heavily in AI, realizing that countries leading in the AI race will enjoy a paradigm shift. In 2017, the CCP's State Council released their strategy for developing AI, entitled "New Generation Artificial Intelligence Development Plan."¹⁹ This strategy outlined China's aims to become the world leader in AI by 2030, to monetize AI into a trillion-yuan (ca. \$150 billion) industry, and to emerge as the driving force in defining ethical norms and standards for AI.²⁰

¹⁹ Roberts, H., *et al.* *The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*, AI & Society (2021). <https://doi.org/10.1007/s00146-020-00992-2>

²⁰ Ibid.

The U.S. has historically been a front-runner in the global AI-race, but China is rapidly closing the gap. For metrics quantifying this gap, please see Appendix 1. These metrics show the U.S. is currently leading in certain key AI metrics, but trends indicate the lead is diminishing.

Another key indicator of progress in AI is a system's performance against technical benchmarks and prize challenges. Producing a top-performing AI system in a particular subfield of AI correlates well with technical leadership in that given subfield of AI. Likewise, if America produces top-performing computer vision systems then America is a leader in state-of-the-art computer vision systems. This has broad implications when recalling the real-world applications associated with subfields of AI. If America produces a top-performing AI system for a particular subfield of AI, it also leads in all of that particular subfield's real-world applications. Ensuring technological leadership in all subfields of AI is critical to maintaining the U.S.'s technological edge over China.

Due to China's data privacy laws, Chinese companies have large data sets to train their AI. In many cases, more data equals better performing AI, creating a competitive advantage for Chinese based AI companies. The U.S. must ethically create and provide access to large, non-sensitive data sets, to fuel progress and improve innovation in AI. A failure to do so will result in Chinese AI, created with non-American values, prevailing on world markets.

b. AUTONOMOUS VEHICLES

To remain the global leader in AVs, the U.S. must enact a federal framework that creates a uniform national standard, expands testing and deployment opportunities by increasing the number of exemptions original equipment manufacturers (OEM) may obtain, and ensure OEMs are not subject to extraneous litigation based around whether features such as entertainment systems function properly. In 2021, the National Highway Traffic Safety Administration (NHTSA) estimated that 42,915 people died in traffic accidents, a 16 year high.²¹ Furthermore, 98% of car crashes are the result of human error.²² The safety benefits AVs promise to deliver by removing the liability of a human driver are clear and well understood, potentially reducing 90% of crash fatalities.²³ It is also clear they are the key to unlocking mobility of the future and ensuring everyone across the country can reap the benefits of safe travel, from people living with disabilities to Americans in both rural and urban areas.²⁴

²¹ National Highway Traffic Safety Administration, *Newly Released Estimates Show Traffic Fatalities Reached a 16-year High in 2021* (May 17, 2022). <https://www.nhtsa.gov/press-releases/early-estimate-2021-traffic-fatalities>

²² U.S. General Services Administration, Office of Motor Vehicle Management, *Crashes Are No Accident*, <https://drivethru.gsa.gov/DRIVERSAFETY/DistractedDrivingPosterA.pdf>

²³ Iyad Rahwan and Azim Shariff, *Self-Driving Cars Could Save Many Lives. But Mental Roadblocks Stand in the Way.*, Wall Street Journal (April 6, 2021). <https://www.wsj.com/articles/self-driving-cars-could-save-many-lives-but-mental-roadblocks-stand-in-the-way-11617732000>

²⁴ National Highway Traffic Safety Administration, *Automated Vehicles for Safety*, <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety>

AVs not only hold vast mobility and safety benefits, they also are projected to spur economic growth – roughly \$8 trillion.²⁵ The deployment of innovative technologies has long been a source of strength for the American automotive sector, supporting 10 million jobs and contributing nearly 3.5 percent to U.S. gross domestic product (GDP).²⁶ Estimates project that annual global revenues from AVs in urban areas could reach \$1.6 trillion by 2030.²⁷

However, these benefits, and security over the supply chain, will only occur if the U. S. leads in the deployment of AVs. The CCP views AVs as a critical part of its future economy, especially to offset labor shortages.²⁸

In 2020, the Chinese central government revealed a plan to have Society of Automotive Engineers (SAE)²⁹ Level 3 autonomous capabilities in 50 percent of all new cars sold by 2025, and 70 percent by 2030.³⁰ The national road map also called for 20 percent of all new vehicles sold to have SAE Level 4 capabilities by 2030.³¹ Additionally, Baidu the operator of China's largest AV fleet, recently received approval to roll out fully driverless vehicles in major cities of Wuhan and Chongqing,³² and plans to deploy more than 3,000 robotaxis in 30 Chinese cities by the end of 2023.³³

Chinese AV companies are conducting research and testing their AVs on American soil, nearly doubling their presence on California roads between 2018 and 2019.³⁴ Chinese companies, like Pony.ai and AutoX, are increasing their testing on California roads, collecting information about Americans and our infrastructure, and subsequently exporting it back to China. American companies who test on Chinese roads are not allowed to send information back to the U.S., as no such data reciprocity exists for American companies.³⁵

²⁵ Michael Wayland, *GM's Cruise Values Autonomous Vehicle Industry at \$8 Trillion*, CNBC (February 5, 2020), <https://www.cnbc.com/2020/02/05/gms-cruise-values-autonomous-vehicle-industry-at-8-trillion.html>

²⁶ Ibid.

²⁷ Hina Miyazu, *Mobility as a Service (MaaS) Market by Latest Trends, Top Key Players, Future Growth, Revenue Forecast, Demand Forecast To 2030*, Comserve (May 11, 2021).

²⁸ Arjun Kharpal, *From Driverless Cars to Robotic Warehouses, China Looks to Automation to Get Ahead of Labor Shortage*, CNBC (May 24, 2021), <https://www.cnbc.com/2021/05/24/china-looks-to-automation-to-solve-population-issues.html>

²⁹ See Appendix 2.

³⁰ Shunsuke Tabeta, *China Wants Self-Driving Tech in Half of All New Cars by 2025*, Nikkei Asia, (November 12, 2020), <https://asia.nikkei.com/Business/Automobiles/China-wants-self-driving-tech-in-half-of-new-cars-by-2025>

³¹ Ibid.

³² CBS News, *Robotaxis are taking over China's roads. Here's how they stack up to the old-fashioned version*, (August 18, 2022), <https://www.cbsnews.com/news/china-robotaxis-self-driving-cabs-taking-over-cbs-test-ride/>

³³ Nicholas Albanese, *Hyperdrive Daily: China Ramps Up its Autonomous Vehicle Development*, Bloomberg (May 4, 2021), <https://www.bloomberg.com/news/newsletters/2021-05-04/hyperdrive-daily-china-ramps-up-its-autonomous-vehicle-development>

³⁴ Shunsuke Tabeta and Takeshi Shiraishi, *China Logs Second-Most Miles in California Self-Driving Tests*, Nikkei Asian (8 Mar. 2019), <https://asia.nikkei.com/Business/China-tech/China-logs-second-most-miles-in-California-self-driving-tests>

³⁵ Translation: Cyberspace Administration of China, *Cyberspace Administration of China Public Comment Notice Regarding Several Provisions on Car Data Security Management*, (May 12, 2021)

The People's Republic of China (PRC) is restricting the use of American AVs in China, expanding Chinese AV presence in the U.S., and explicitly outlining a goal of surpassing the U.S. leadership in this technology.³⁶ Despite the unanimous House passage of the SELF DRIVE Act in 2017, Congress has failed to enact a law and the U.S. currently risks ceding leadership to the CCP. It would be a catastrophic societal and economic loss for the American automotive and tech sectors, the country, and Americans to lose this market due to Congressional inaction.

c. BLOCKCHAIN

A blockchain is a distributed, consensus-driven, immutable ledger for recording information. Many blockchains build in democratic principles like privacy and autonomy into the foundation of their technology, ultimately leading to the PRC's ban on privately controlled blockchains in 2021.³⁷

Blockchains are a central component of the CCP's strategy to undermine the U.S.-led global order. In 2019, the CCP established the Blockchain-based Service Network (BSN).³⁸ BSN is a low-cost blockchain surveillance layer that sits at the bottom of a blockchain foundation enabling the Chinese government to compromise and exploit large pools of data that should otherwise be private. Should BSN become a global standard, the CCP would be able to monitor the identities and data of all global users.³⁹ Tan Min, BSN Secretary General, stated that BSN would build an internet where "China controls the rights to internet access."⁴⁰ The BSN standard is already seeing adoption in multiple countries besides mainland China, and becomes increasingly alarming as the CCP prepares to pair the technology with its digital Belt and Road Initiative.⁴¹

The U.S. must develop a nation-wide strategy for promoting the use of blockchain-based infrastructures to ensure China does not control the world's rights to access the internet. Despite the dominance of Silicon Valley during the early days of the internet, only 40% of blockchain companies are headquartered in the U.S.⁴² The U.S. needs to incentivize the creation of a vibrant private sector blockchain ecosystem in order to beat the CCP's centralized and surveillance-based model.

³⁶ Xinhua, *Full Text: Sustainable Development of Transport in China*, (December 22, 2020).

³⁷ Alun John, Samuel Shen, Tom Wilson, *China's Top Regulators Ban Crypto Trading and Mining, Sending Bitcoin Tumbling*, Reuters (September 24, 2021). <https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/>

³⁸ Ledger Insights, *China's national blockchain infrastructure takes shape* (December 2, 2019) <https://www.ledgerinsights.com/chinas-national-blockchain-infrastructure-bsn/>.

³⁹ Yao Qian, *Technical Aspects of CBDC in a Two-Tiered System*, Institute of Digital Money, People's Bank of China (July 7, 2018) <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180718/Documents/Yao%20Qian.pdf>

⁴⁰ 24 minute mark, "How Blockchain Technology and BSN Support Fintech Development," *YouTube*, November 4, 2020. https://www.youtube.com/watch?v=k9Gtq-j_3U

⁴¹ Mikk Raud, *Knowledge Base: Blockchain-based Service Network*, DigiChina (July 2, 2021) <https://digichina.stanford.edu/work/knowledge-base-blockchain-based-service-network-bsn-%E5%8C%BA%E5%9D%97%E9%93%BE%E6%9C%8D%E5%8A%A1%E7%BD%91%E7%BB%9C/>

⁴² PitchBook (n.d.) *Companies in Blockchain and Cryptocurrency*. PitchBook

E. SUPPLY CHAIN

The dependency of American supply chains on the PRC creates opportunities for significant disruption by the CCP. The COVID-19 pandemic and subsequent supply chain shocks exposed the vulnerabilities of U.S. supply chains and the dangers of over reliance on the PRC. The U.S. cannot outspend the CCP in the hopes of securing our supply chains. Duplicative billion-dollar programs will further bury the U.S. behind bureaucratic red tape of permitting requests by companies seeking to access critical minerals in the U.S. or build leading-edge manufacturing facilities here at home.

The U.S. must enact regulatory frameworks attractive to retaining and growing domestic supply chains, so supply chains are resilient to the shocks we saw in 2021 and eliminate vulnerabilities to Chinese abuse. Companies, and trade partners of the U.S., should examine other manufacturing and raw material suppliers to ensure the security of supply chains. Moving such processes to nations with shared values must happen to ensure self-reliance among countries that share values with the U.S.

IV. Relevant Committee Action

A. American COMPETE Act

In 2020, Congress passed, and the President signed into law, The American Competitiveness of a More Productive Emerging Tech Economy Act (American COMPETE). This law requires the Department of Commerce (DOC) and the Federal Trade Commission (FTC) to study and submit reports to Congress related to how the emerging technologies can create economic benefits in the U.S. and how the U.S. can create a competitive environment to advance the deployment of such technologies. Specifically, the legislation required the DOC and the FTC to examine:

- AI
- IOT in manufacturing
- Quantum Computing
- Blockchain Technology
- New and Advanced Materials
- Unmanned Delivery Systems
- IOT
- Three-Dimensional printing
- How to combat harms through innovation

V. ISSUES

- What are the national and economic security threats of China leading in the deployment of emerging technologies like AVs?
- What becomes of the U.S. economic vitality if China establishes global standards for emerging technologies?
- How can the U.S. implement policies that reduce barriers to AV development in a way that is consistent with U.S. values?
- What dangers persist to Americans if the CCP is able to easily access their sensitive information?
 - Why is passing a national privacy and data security law necessary to protect American's sensitive information from the CCP?
 - How will Congressional inaction on passing a national privacy and data security law, hamper innovation and entrepreneurship in the U.S.?
 - How can the U.S. government use incentives to ensure that U.S. companies are not entering into agreements, with Chinese companies, that leave American's data exposed?
- What regulatory challenges exist at the federal, state, or local level to deploying new emerging technologies?
 - How can the U.S. enact policies, or reduce red tape, to ensure that these technologies are developed in the U.S. and not in China?
 - How can the U.S. ensure that components in emerging technologies are not vulnerable to unfavorable data sharing agreements with manufacturers and retailers from China?
- What role can agencies like the DOC serve in the promotion of American leadership in emerging technologies?
- How will future technologies change if countries like China are allowed to lead in their global development?

VI. STAFF CONTACTS

- Tim Kurth, Chief Counsel
- Teddy Tanzer, Senior Counsel
- Brannon Rains, Professional Staff Member
- Michael Cameron, Professional Staff Member
- Lacey Strahm, Technology Fellow
- Jessica Herron, Clerk

APPENDIX 1

U.S.-China AI Activity Metrics

AI Activity Metrics (2021)	United States	China
Journal Publications	13.67% of the global share	31.04% of the global share [+1]
Citations of Journal Publications	17.45% of the global share	27.84% of the global share [+1]
Repository Publications	32.52% of the global share [+1]	16.60% of the global share
Citations of Repository Publications	38.60% of the global share [+1]	16.4% of the global share
Conference Publications	16.90% of the global share	27.64% of the global share [+1]
Conference Citations	29.52% of the global share [+1]	15.32% of the global share
Patent Filings	16.92% of the global share	51.69% of the global share [+1]
Patents Granted	39.59% of the global share [+1]	5.90% of the global share
Private Investment	\$52.88B [+1] \$149B (2013-2021) [+1] Databricks leads.	\$17.2B \$61.9B (2013-2021) Beijing Horizon Robotics Technology leads.
Newly Funded Companies	299 companies [+1] 3,234 companies (2013-2021) [+1]	119 companies 940 companies (2013-2021)
Hiring Index	1.17	1.18 [+1]
Skill Penetration	2.24 [+1]	1.56
Bills Passed into Law	13 (2016-2021) [+1]	2 (2016-2021)
Total	10	5

** Unless otherwise indicated, these numbers are static representations of data from the year 2021 pulled from the AI Index Report 2022⁴³. To better understand year-over-year trends please see Figure 1.1.10–1.1.24c, Figure 4.1.1-4.1.8, Figure 4.2.2–4.2.9., and Figure 5.1.2b of the AI Index Report 2022.*

⁴³ Daniel Zhang, et. al., *The AI Index 2022 Annual Report*, AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University, (March 2022). <https://aiindex.stanford.edu/report/>

APPENDIX 2

SAE J3016 Levels of Driving Automation



SAE J3016™ LEVELS OF DRIVING AUTOMATION™

Learn more here: [sae.org/standards/content/j3016_202104](https://www.sae.org/standards/content/j3016_202104)

Copyright © 2021 SAE International. The summary table may be freely copied and distributed AS-IS provided that SAE International is acknowledged as the source of the content.

	SAE LEVEL 0™	SAE LEVEL 1™	SAE LEVEL 2™	SAE LEVEL 3™	SAE LEVEL 4™	SAE LEVEL 5™
What does the human in the driver's seat have to do?	You are driving whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			You are not driving when these automated driving features are engaged – even if you are seated in “the driver's seat”		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	

Copyright © 2021 SAE International.

	These are driver support features			These are automated driving features	
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/acceleration support to the driver	These features provide steering AND brake/acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met	This feature can drive the vehicle under all conditions
Example Features	<ul style="list-style-type: none"> • automatic emergency braking • blind spot warning • lane departure warning 	<ul style="list-style-type: none"> • lane centering OR • adaptive cruise control 	<ul style="list-style-type: none"> • lane centering AND • adaptive cruise control at the same time 	<ul style="list-style-type: none"> • traffic jam chauffeur 	<ul style="list-style-type: none"> • local driverless taxi • pedals/steering wheel may or may not be installed • same as level 4, but feature can drive everywhere in all conditions